Enlighten Information Morals through Corporate Culture

A. Alumubark, N. Hatanaka, O. Uchida and Y. Ikeda

Graduate School of Informatics
Tokyo University of Information Sciences, Chiba, Japan
e-mail : h14001aa@edu.tuis.ac.jp; {hatanaka, o-uchida, ikeyuki}@rsch.tuis.ac.jp

Abstract

The leakage of secret information has increasingly become a social problem. Information leaks typically result from the targeting of specific organizations or persons and are based on a variety of factors. One factor common to the majority of leaks is the relationship between corporate culture and information morals. Organizations that lack robust standards of information morals are at a greater risk of information leaks. This paper aims to identify the causes of information leaks by applying organization theory and statistical analysis to assess the impact of corporate culture on information leaks and information morals. Furthermore, the relationship between organizational objectives and social values is discussed in order to propose a clear assessment process of corporate culture.

Keywords

Information Morals, Information Security, Security Incidents

1. Introduction

Information security begins and ends with people, while incidents and accidents involving the leakage of personally identifiable information show no sign of significant decline, e.g. the Dai Nippon Printing Co., Ltd. and the Benesse Holdings, Inc. leakage incidents. In order to understand the cause of information leaks, it is necessary to investigate the relationship between individuals and organizations. The research presented will assess the impact of corporate culture on information security incidents, information morals and the interrelationship between people and organizations. This research will also reveal that information security incidents are attributed to unaddressed information security vulnerabilities and the disharmony between organizational objectives and social values. This paper will then propose how to improve information morals through corporate culture.

2. Lack of Function Concerning Information Morals

Increasing information security is a challenge. Many organizations protect their information assets by focusing on security breaches and extended expenses related to security technologies; however, it is impossible to eliminate incidents and accidents simply by applying security technologies. It is important to identify other factors that generate incidents and accidents in the organization. There exists a widespread

disconnect between the people that comprise organizational structures and the standards of information morals established by the organization. Previous research on this issue have focused on some features of corporate culture, however most of them have not succeed to identify the causes of information security incidents and improve information morals through corporate culture.

In this research, identify the defects of corporate culture that contribute to information security incidents and propose an assessment process to improve information morals within an organization. The goals of this paper are as follows:

- Determine the effects of corporate culture on information security incidents.
- Describe the impact of organizational hierarchy on corporate culture.
- Describe the impact of corporate culture on information morals.
- Establish a process for the assessment of corporate culture and its impact on information morals.

The research procedure was as follows:

- Develop a survey questionnaire concerning with information morals and corporate culture.
- Apply covariance structure analysis to extract factors of corporate culture from survey data through an exploratory factor analysis.
- Induce (variables) concerned with the organizational variable.

3. The Defects of Hierarchical Organization

Barnard (1938) studied the strengths and weakness of hierarchical organizational structures. He considered that the strengths of the hierarchical organizational structure related to the ability of leaders and swift actions. Those factors lead the hierarchical organization to success in the Industrial Age. He considered the weaknesses to be disparities in the distribution of wages and prestige among different positions, which lowered employee morale. He called those shortcomings "the inverse function of the hierarchical organizational structure" and considered them to be a major cause of scandals and accidents. The following points ought to be considered as defects of the status system and the hierarchical organization.

1. Deficiencies in the Status System (Barnard, 1938)
    - Hierarchies distort the true value of individuals in a status system.
    - The circulation of the position of the elite is unfairly limited; the ability to strengthen the exclusive positions by a specific person becomes a problem.
    - The system of distribution, such as equitable positions, functions, and responsibilities, is distorted; there is discrimination in the distribution of wages, honor, and prestige based on status.

2. Deficiencies in the Hierarchy (Barnard, 1938)
    - The administrative functions are exaggerated, and the function of morals is hampered.
    - It is an excessive symbolization function. The major issue is that the status and the true value of individuals are often confused.
    - Though it is indispensable in the cohesiveness and coordination of organizations, the hierarchy reduces the resilience and adaptability of organizations.

Barnard (1938) presented an organizational structure involving multiple layers of subcontractors as a "lateral organization," which referred to collaboration as a whole, without any formal upper-level organizations or leaders (Mano, 1989). He categorized the lateral organization into shareholders, creditors, consumers, raw material suppliers, and local governments, and subcontractors fall within the category of raw material suppliers. Furthermore, he emphasized that it is also possible to prevent information security incidents and accidents through the practical application of the lateral organization.

3.1. Sympathizing with Corporate Objectives and Social Values

Simon (1945) considers against the productivity of concept, which is determined by the relationship between the inputs and outputs of Taylorism, that organizations can increase their value, prevent corporate incidents and scandals, and increase the loyalty of their employees only when their objectives and social values are consonant. In the cases of Dai Nippon Printing Co., and Benesse Corp., the information security incidents occurred due to disharmony between social values and organizational objectives within a hierarchical structure.

3.2. The Organizational Cause of Incidents

The "administrative principles" of the organization were presented by Simon (1945). They relate to the challenges organizations face while resolving incidents. By comprehensively considering the following points, it is conceivable that suggestions can be obtained for improving efficiency and preventing organizational incidents.

Administrative efficiency is increased by the following:

1. By specializing works in a group.
2. By arranging the members to the hierarchy of the authority.
3. By limiting the span of control at small numbers of persons at any level of the hierarchy.
4. By grouping the employees according to the sort of work they do.

Consideration must be given, however, to the adverse affects of those factors since they cause organizational incidents. Nevertheless, those factors do correlate positively with efficiency. In other words, overall business efficiency results from improvements in organizational efficiency and productivity. Considering that the

organization can be a hotbed of incidents, it appears necessary to confirm not only the activities and the decision-making of the organization, but also the effectiveness and the limitation of the hierarchy as in the collaboration method.

The similarities between scandals and incidents were observed through the collected data on 140 Japanese organizations in which information security incidents took place from 2006 to 2014. The data were collected from reliable websites in Japan, IPA`s archives (Information Technology Promotion Agency), and investigated these incidents cause with (Simon 1945) suggestions. It was seen that similar scandals and incidents had similar causes, the cause by social value or corporate culture.

4. The Relationship between Corporate Culture, Information Morals, and Information Security Incidents

Hofstede (2010) considers culture to be comprised of two primary elements. "Culture one" is comprised of civilization, or "refinement of the mind," and encompasses elements of society and culture such as education, literature, and art. "Culture two" is a broader conception of the word, and is related to the patterns of thinking, feeling, and acting in which individuals engage. Individuals living and operating within the same social environment tend to share these elements.

Shover and Hochstetler (2002) found that variations within the culture of an organization affect many elements of organizational performance. These include effectiveness in goal attainment and failing to comply with approved standards of conduct. Generally, there is high intra-organizational cultural uniformity. Thus, whether failing to comply with standards or legitimate, such behaviors reinforce one another (Shover & Hochstetler 2002). In line with these findings, Da Veiga and Eloff (2010) assert that an organization's approach to information security must focus on the moral behavior of employees. Gebrasilase and Lessa (2011) state that information security culture is comprised of a set of information security characteristics that are valued by the entirety of the organization. This emphasizes the effect that corporate culture has on the information morals of employees.

Van Niekerk and Von Solms (2010) researched information asset security and found that, whether due to negligence or intent, employees are its greatest threat. To ensure against the threat of negligence, it is essential that organizations establish a culture of information security and clear information morals. By establishing those standards, human factors that generate risk to information security are minimized and managed. The accomplishment of this goal, however, is not so simple (Alfawaz, 2010). Alfawaz (2010) noted the difficulty in understanding the complex, dynamic, and uncertain characteristics related to employees who perform information security activities, whether authorized or unauthorized. Information security management is influenced by individual and group behaviours alike, and must be managed as such.

Modern business and industry experts have increasingly demanded a stronger focus on information security. Information security must be incorporated into organizational strategies to be effectively addressed, but there is no clear blueprint

through which a firm may achieve a corporate structure that supports organizational culture (Kayworth & Whitten, 2010). The values that are associated with organizational culture are manifested in the practices and activities within the organization in relation to information security management (Alfawaz et. al., 2010).

Focusing on information security within organizations is a comprehensive process. Kayworth and Whitten (2010) conducted qualitative research comprised of interviewing 21 information security executives from 11 organizations, and found that information security strategies are complex. Generally, those strategies incorporate not only IT products and solutions, but also social alignment and organizational integration mechanisms. The strategies are often managed through the institution of a control-based compliance model (Hedstrom, 2011).

Mitigation of information security threats depends on determining their sources. Often, such threats stem from organizational insiders. Insiders can cause greater damage due to their position; thus, they must be identified and subsequently targeted by countermeasures. Information security countermeasure strategies are a means of addressing particular threats (Coles-Kemp, 2010). The socio-technical approach is a means to achieve three objectives: achieving a balance between security essentials and the need to enable the business, maintaining compliance, and ensuring that the strategy is appropriate for the organizational culture (Kayworth &Whitten, 2010).

Employees are central to the protection of organizational information, which has prompted the study of so-called "security culture." By embedding security culture into the corporate culture, employee behaviors that protect the information of the organization are positively influenced (Lim, 2010). This positive reinforcement of moral behavior helps to lower the risk of information leaks. Employee compliance is one of the more difficult facets of information security, highlighting the importance of enforcement. One way to directly control and observe employee behavior in relation to information security is by monitoring employee computers (Green & D'Arcy, 2010). To measure employee behavior related to information security, Padayachee (2012) studied the extrinsic and intrinsic motivations that influenced employees' propensity to compliant information security behavior. Employee behavior in this regard is comprised of a set of core information security activities that must be adhered to by end-users to promote security.

5. Factors Influencing Corporate Culture and Information Morals

Covariance structure analysis was applied for comparisons through statistical testing of the effects of the latent variables (corporate cultural type) on the observed variables. Factors and issues related to scandals were proposed by the research group at Hitotsubashi University (Hoshino, 2008). While there are already case studies that have discussed scandals within organizations in Japan, we attempted to use these factors to explain the similarities between information incidents and scandals.

5.1. Questionnaire Design

A questionnaire for an IT department of IMAM institute in Tokyo was developed in both Japanese and English format. The distribution method was in site of IMAM institute and it was conducted in 8 November 2014. 184 answers were received, the sample details of the survey results shown in Table 1. The survey consisted of two parts. Part one, gathered information on employee demographics, using multiple-choice questions that allowed the researcher to examine such factors as department age, job duties, and background of information security experience. In part two, 43 observed variables were classified into eight categories. The observed variables concerned with the section "Culture of fraud and neglect of violation in the workplace" were measured on a 5-point Likert scale (1: None, to 5: Frequently). Other observed variables were measured on a 5-point scale (1: Disagree, to 5: Agree).

Participant's Answers		100%
Participant's age	20 or under	3
	21 – 30	24
	31 – 40	37
	41 – 50	31
	51 – 60	5
Participant's gender	Male	81
	Female	19
Job duties	Leader	1
	Manager	2
	Employer	91
	Contractor	6
Education level	Graduate School	48
	Collage	43
	Other	9
I have violated by a virus to my computer		78
I have looked into a password of another person		36
I have shared my password to another person		14

Table 1: Summary of survey results

5.2. Exploratory Factor Analysis

An exploratory factor analysis was applied to extract factors. Eight factors were extracted from the 43 observed variables. All coefficient alpha values were more than 0.8, which indicates that observed variables were positive. Through the results of the exploratory factor analysis, variables concerned with information security incidents have been induced. Results are shown in Table 3 and 4. The results indicate that all eight factors are valid for confirmatory factor analysis.

Latent variables	Number of Questions	Contribution Ratio	Coefficient Alpha
Culture of fraud and neglect of violation	8	0.846	0.802
Trust in the workplace	5	0.875	0.820
Sectarian behavior	9	0.906	0.905
Belonging scale	5	0.856	0.811
Moral leadership	3	0.676	0.894
Leadership at the workplace level	4	0.718	0.894
Development of compliance system	3	0.618	0.827
Other single indicators	6	0.862	0.849

Table 2: Summary of exploratory factor analysis

	Factor							
	1	2	3	4	5	6	7	8
Compliance7	**.911**	.065	.026	.061	-.059	.011	-.019	-.084
Compliance6	**.884**	-.020	-.070	-.014	.048	.004	-.035	.055
Compliance5	**.651**	-.037	.017	-.077	.005	.190	.114	-.069
Trust1	.023	**.826**	-.029	.062	.007	-.014	-.002	-.066
Trust3	.021	**.821**	.015	-.004	-.010	-.070	.040	.031
Trust4	-.029	**.749**	-.008	-.053	.016	.081	-.016	.121
Belonging4	-.185	.055	**.875**	-.017	-.040	.074	.040	-.036
Belonging5	.119	.033	**.850**	-.015	.026	-.015	-.030	-.064
Belonging3	.049	-.135	**.742**	.045	.032	-.061	.018	.156
Sectarian7	-.081	-.052	-.073	**.901**	.024	.084	.129	-.034
Sectarian6	.113	-.010	.144	**.814**	-.029	-.067	-.083	.029
Sectarian2	-.020	.082	.009	**.771**	.041	-.008	-.067	.026
Culture_fraud3	.026	-.007	.001	-.087	**.963**	.033	-.057	-.014
Culture_fraud2	-.006	-.063	-.069	.117	**.654**	-.076	.085	.153
Culture_fraud7	-.039	.102	.095	.056	**.560**	.029	-.005	-.177
Moral2	.045	-.001	.006	.052	.010	**.821**	.117	.027
Moral3	.112	-.011	.002	-.018	-.018	**.812**	-.101	.122
Other3	.015	.000	.010	.034	.008	.085	**.890**	-.114
Other1	.196	.066	.023	-.061	-.004	-.168	**.537**	.234
Leadership4	-.044	.075	.025	.014	-.007	.160	-.037	**.752**

(Extraction Method: Principal Axis Factoring)

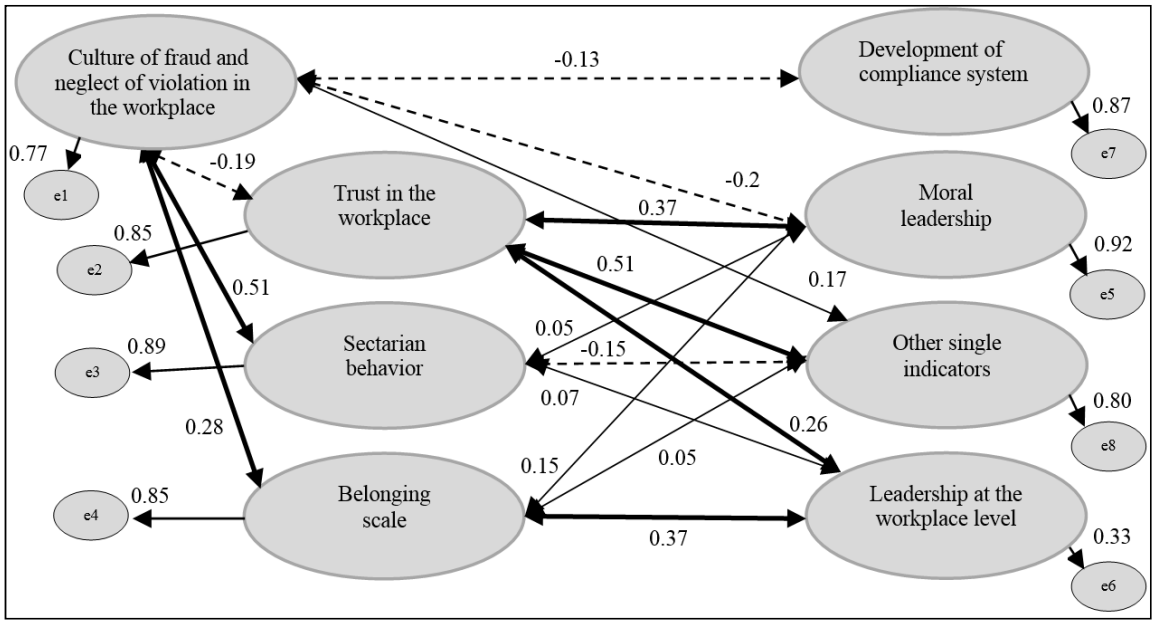
Table 3: Results of exploratory factor analysis

No	Induced Variables
1	Have you ever made false reports in your workplace?
2	The information transfer between members is performed widely and smoothly.
3	The subordinate who does not give a present (gift) to the manager has a disadvantage regarding promotions.
4	When incidents or accidents occur, the concern is more of "whose responsibility it is" than of "what the cause is."
5	The managers in my workplace behave as a moral model for others.
6	The manager shows enough leadership at work.
7	I am aiming to establish a compliance (legal and ethical compliance).
8	The work objective of each person is clear every day.

Table 4; Results of induced variables

5.3. Confirmatory Factor Analysis

The results of the confirmatory factor analysis were induced and are shown in Figures 1. As a result, the most influential are “Sectarian behaviour” and “Belonging scale.” The more “sectarian behaviour” increases, the higher “culture of fraud and neglect of violation in the workplace” rises. Furthermore, the greater level of “moral leadership” demonstrated by the administration, in combination with an increase in “trust in the workplace,” the lower “culture of fraud and neglect of violation in the workplace” becomes. It also shows that “other single indicators” give certain effects, but the influence is small compared to the variables mentioned above. In addition, it has been shown that “culture of fraud and neglect of violation in the workplace” decreases in organizations that score higher in “development of compliance system.” Its influence, however, is limited.



(GFI= 0.915, CFI= 0.971, RMSEA = 0.035)

Figure 1: Result of confirmatory factor analysis

6. Improvement of Information Morals

In order to launch assessments of information security incidents and improve the standards of information morals, the designer of the organizational structure must specify the elements and aspects of corporate structure that may improve or degrade corporate culture. Next, the designer or planner evaluates and supposes the change to the aspects of corporate culture. This process is proposed as "the assessment process of corporate culture." For example, consider an employee in an IT department who lost a USB containing sensitive information. In this case, the employee lost the confidence of customers by failing to consider the importance of protecting customers' information. The employee did not uphold the moral duty to protect customers' personal data. This had the effect of degrading the department`s corporate culture. Thus, it was necessary for the department's management to educate and discipline that employee. The above illustration is shown in the assessment process of corporate culture in Table 5. The proposed assessment process is as follows:

Process 1 Specifying and identifying the elements and corporate culture aspects that characterize the organization.

Process 2 Assessing and supposing the change to corporate culture after organizations activities.

Process 3 Establishing the objectives induced from and consistent with organizational policy by management.

Process 4 Setting measurable targets that are induced from the objective itself.

Process 5 Measuring the performance of the organization's activities.

	Past	Present					Future
Organization	Incidents	Aspect		Impact	Objectives	Target	Performance
IMAM Inst, IT Dept	An employee lost his USB memory contains information (Name, Address, Contact numbers)	Agent	The employee has not awareness of the importancy of job's information.	The employee disregards the leak of job's information	The employee aware that the job's information is protected from missing or losing.	Limit the amount of confidential information stored on portable medium (USB) to only the minimum necessary. Itself to achieve level is 80%.	The employee takes into consideration the importance of protecting job's information. Performance level is 25%.
		Organization's Objectives	The objectives are ambiguity, not acceptable by organization members, itself not to achieve, lack of information security, etc.	The employee has not the responsibility to the job duty, comply with organization policy, etc.	Management sets a policy as job's information are not leaked out of the organization.	Each member of IT deparment required to read and understand the information security policy. Itself to achieve level is 100%.	The employee contributing to his deparment, and has awareness of deparment strategies. Performance level is 70%.
		Management	The management has not invest the equipment and the training program to employee, enlightenment activities.	The unwanted and unexpected events which are suddenly occurred in the organization leaved alone.	Management invest the budget. Maked policy are well-known, and understood.	Each member of IT deparment required to attend the training program, frequently measure the response of staff with the awareness program. Itself to achieve level is 100%.	Management take secret information seriously also takes the necessary awareness or training program. Performance level is 90%.
		Interaction between Agents	Management and employee did not share the organizational value.	The shared organizational value are degrade, collapsed, etc.	The shared organizational value will be improved.	The information of unwanted and unexpected events are provided through the hierarchy, interaction between agents. Itself to achieve level is 100%.	The information of unwanted and unexpected events are provide. Performance level is 20%.

Table 5. Assessment Process of Corporate Culture

7. Conclusion

Prevention of information security incidents within the organization has become a very important topic. In this research, moral concerns of corporate culture have been operationally defined by a questionnaire. By utilizing the survey data, it was investigated how factors that influence information morals in the workplace can be affected by management actions and the overall corporate structure.

The results showed that sectarian behaviour, belonging scale, moral leadership, and other single indicators have a powerful influence on corporate culture and moral behavior. Development of compliance systems has only a limited effect on the culture of fraud and neglect of violation in the workplace, and it does not have a very strong influence on information morals.

An assessment process of corporate culture has been proposed in order to maintain high standards of information morals and prevent incidents such as information leaks. The process has been made visible by showing how to create the table included herein as Table 5. Through the application of this assessment process, one

may discover areas of corporate culture that adversely affect the standards of information morals within the organization.

8. References

Alfawaz, S., Nelson, K., & Mohannak, K. (2010, January). Information security culture: a behavior compliance conceptual framework. In *Proceedings of the Eighth Australasian Conference on Information Security*, Volume 105 (pp. 47-55).

Barnard, I., "The Functions of the Executive.", *Harvard University Press*, 1938.

Coles-Kemp, L., & Theoharidou, M. (2010). Insider threat and information security management. *In Insider Threats in Cyber Security* (pp. 45-71). Springer US.

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196-207.

Gebrasilase, T., & Lessa, L. F. (2011). Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital. *The African Journal of Information Systems*, 3(3), 1.

Greene, G., & D'Arcy, J. (2010, June). Assessing the Impact of Security Culture and the Employee-Organization Relationship on IS Security Compliance. In *5th annual symposium on information assurance* (ASIA'10) (p. 1).

Hedstrom, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems*, 20(4), 373-384.

Hofstede, G. (2010). Culture and Organizations: Software of the Mind. *New York, NY: McGraw-Hill*.

Hoshino, T., Arai, K., Hirano, S., & Yanagisawa, H. (2008). An empirical analysis of organizational climates of misconduct. *Hitotsubashi University*, 2(2): 157-177.

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS Quarterly Executive*, 9(3), 2012-52.

Lim, J. S., Ahmad, A., Chang, S., & Maynard, S. (2010). Embedding information security culture emerging concerns and challenges. *PACIS 2010 Proceedings*, Paper 43.

Mano, "The Meaning of the Concept of Lateral Organization in C.I. Barnard's Theory", *Hokkaido University Economic Studies*, 39-1, June, 1989.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security*, 31(5), 673-680.

Shover, N., & Hochstetler, A. (2002). Cultural explanation and organizational crime. *Crime, Law, & Social Change*, 37, 1-18.

Simon, H. A., "Administrative Behavior", *The Free Press*, 1945.

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, 29(4), 476-486.